

# RECOMPOSING RATIONAL FUNCTIONS

FEDOR PAKOVICH

**ABSTRACT.** Let  $A$  be a rational function. For any decomposition  $A = V \circ U$  of  $A$  into a composition of rational functions  $U$  and  $V$ , the rational function  $\tilde{A} = U \circ V$  is called an elementary transformation of  $A$ , and rational functions  $A$  and  $B$  are called equivalent if there exists a chain of elementary transformations between  $A$  and  $B$ . This equivalence relation naturally appears in the complex dynamics as a part of the problem of describing of semiconjugate rational functions. In this paper we show that for a rational function  $A$  its equivalence class  $[A]$  contains infinitely many conjugacy classes if and only if  $A$  is a flexible Lattès map. As a case study we consider in details flexible Lattès maps  $\mathcal{L} = \mathcal{L}_j$  induced by the multiplication by 2 on elliptic curves with corresponding  $j$ -invariant. In particular, we show that any rational function equivalent to  $\mathcal{L}_j$  necessarily has the form  $\mathcal{L}_{j'}$  for some  $j' \in \mathbb{C}$ , and that conjugacy classes in  $[\mathcal{L}_j]$  can be identified with orbits of  $j$  under the correspondence associated with the classical modular curve  $\Phi_2(x, y) = 0$ .

## 1. INTRODUCTION

Let  $B$  be a rational function of degree at least two. The function  $B$  is called semiconjugate to a rational function  $A$  if the equality

$$A \circ X = X \circ B \tag{1}$$

holds for some rational function  $X$ . In case if  $X$  is invertible,  $A$  and  $B$  are called conjugate. In terms of dynamical systems condition (1) means that the dynamical system  $A^{\circ k}$ ,  $k \geq 1$ , on  $\mathbb{CP}^1$  is a factor of the dynamical system  $B^{\circ k}$ ,  $k \geq 1$ . The semiconjugacy is not a symmetric relation. However, if  $B$  is semiconjugate to  $A$ , and  $C$  is semiconjugate to  $B$ , then  $C$  is semiconjugate to  $A$ , since equalities (1) and  $B \circ W = W \circ C$  imply the equality

$$A \circ (X \circ W) = (X \circ W) \circ C.$$

In the recent paper [9] equation (1) was investigated at length. Roughly speaking, the main result of [9] states that (1) holds in two cases. In the first case, the corresponding functions  $A$  and  $B$  are either Lattès maps, or functions which can be considered as analogues of Lattès maps related to automorphism groups of  $\mathbb{CP}^1$  instead of automorphism groups of  $\mathbb{C}$ . In the second case, the functions  $A$  and  $B$  do not possess any special properties, however they are *equivalent* with respect to an equivalence relation  $\sim$  on the set of rational functions defined as follows. For any decomposition  $A = V \circ U$ , where  $V$  and  $U$  are rational functions, the rational function  $\tilde{A} = U \circ V$  is called an elementary transformation of  $A$ , and rational functions  $A$  and  $B$  are called equivalent if there exists a chain of elementary transformations between  $A$  and  $B$ . For a rational function  $A$  we will denote its equivalence class by  $[A]$ .

The connection between the relation  $\sim$  and semiconjugacy is straightforward. For  $\tilde{A}$  and  $A$  as above we have:

$$\tilde{A} \circ U = U \circ A, \quad \text{and} \quad A \circ V = V \circ \tilde{A},$$

implying inductively that whenever  $A \sim B$  there exist  $X$  such that (1) holds, and  $Y$  such that

$$B \circ Y = Y \circ A$$

holds. Therefore, if  $A \sim B$ , then each of the dynamical systems  $A^{\circ k}$ ,  $k \geq 1$ , and  $B^{\circ k}$ ,  $k \geq 1$ , is a factor of the other one, meaning that these systems have “similar” dynamics. Furthermore, since for any invertible rational function  $W$  the equality  $B = (B \circ W) \circ W^{-1}$  holds, each equivalence class is a union of conjugacy classes. Thus, the relation  $\sim$  can be considered as a weaker form of the classical conjugacy relation.

The main result of this paper is the following statement providing a characterization of flexible Lattès maps in terms of the above equivalence relation.

**Theorem 1.1.** *Let  $A$  be a rational function. Then its equivalence class  $[A]$  contains infinitely many conjugacy classes if and only if  $A$  is a flexible Lattès map.*

Simplest examples of flexible Lattès maps, considered in this paper as a case study, are rational functions  $\mathcal{L}$  induced by the multiplication by 2 on elliptic curves. Such a function can be defined by the equality

$$\wp(2z) = \mathcal{L} \circ \wp(z), \quad (2)$$

where  $\wp(z)$  is the Weierstrass function associated with some lattice  $M$  of rank two in  $\mathbb{C}$ . Two such functions corresponding to lattices  $M$  and  $M'$  are conjugated if and only if the elliptic curves  $\mathbb{C}/M$  and  $\mathbb{C}/M'$  are isomorphic. So, abusing the notation, we will denote by  $\mathcal{L}_j$  any Lattès map induced by the multiplication by 2 on an elliptic curve with given  $j$ -invariant.

In order to see all conjugacy classes in  $[\mathcal{L}_j]$  “at once” it is convenient to use the notion of correspondence  $\mathcal{F}$  associated with an affine algebraic curve  $F(x, y) = 0$ . By definition, for  $x_0 \in \mathbb{C}$  the image of  $x_0$  under  $\mathcal{F}$  is any point  $y_0 \in \mathbb{C}$  such that  $F(x_0, y_0) = 0$ . More generally,  $y_0 \in \mathbb{C}$  is the image of  $x_0 \in \mathbb{C}$  under the  $k$ th iteration of  $\mathcal{F}$  if there exists a sequence  $x_0, x_1, \dots, x_k = y_0$  such that  $(x_{i-1}, x_i)$ ,  $i = 1, \dots, k$ , is a point on  $F(x, y) = 0$ . Considering the totalities of all images and preimages of a point  $x_0$  we can define its forward, backwards, and full orbit under  $\mathcal{F}$ . If  $F(x, y)$  is symmetric, that is  $F(x, y) = F(y, x)$ , all these orbits coincide, so we can use simply the term orbit. Under the above notation the following statement holds.

**Theorem 1.2.** *Let  $\mathcal{L}_j$ ,  $j \in \mathbb{C}$ . Then any rational function  $B$  such that  $B \sim \mathcal{L}_j$  has the form  $B = \mathcal{L}_{j'}$ ,  $j' \in \mathbb{C}$ , and conjugacy classes in  $[\mathcal{L}_j]$  can be identified with elements of the orbit of  $j$  under the correspondence associated with the classical modular curve  $\Phi_2(x, y) = 0$ .*

Notice that although the curve  $\Phi_2(x, y) = 0$  is quite bulky it has a very simple parametrization by rational functions which goes back to Klein ([1]), implying that  $\mathcal{L}_{j'} \sim \mathcal{L}_j$  if and only if  $j$  and  $j'$  are in the same orbit of the multivalued function

$$\mathcal{F} = \beta \circ \frac{1}{z} \circ \beta^{-1}, \quad (3)$$

where  $\beta$  is a rational function of degree three,

$$\beta(z) = 64 \frac{(z+4)^3}{z^2}.$$

The paper has the following structure. In the second section we show that the condition  $A \sim B$  implies that  $A$  and  $B$  are isospectral, and deduce the “only if” part of Theorem 1.1 from the fundamental result of McMullen ([3]) about isospectral rational functions. In the third section we first study functions  $\mathcal{L}_i$  and prove Theorem 1.2. Then we prove “if” part of Theorem 1.1 for arbitrary flexible Lattès maps.

## 2. EQUIVALENCE AND ISOSPECTRALITY

Recall that a rational function  $A$  is called a *flexible Lattès map* if there exist an elliptic curve  $\mathcal{C}$  and morphisms  $\varphi : \mathcal{C} \rightarrow \mathcal{C}$  and  $\pi : \mathcal{C} \rightarrow \mathbb{CP}^1$  such that the diagram

$$\begin{array}{ccc} \mathcal{C} & \xrightarrow{\varphi} & \mathcal{C} \\ \downarrow \pi & & \downarrow \pi \\ \mathbb{CP}^1 & \xrightarrow{A} & \mathbb{CP}^1, \end{array} \quad (4)$$

is commutative,  $\pi$  has degree two, and  $\varphi$  has the form  $\varphi = \alpha z + \beta$ , where  $\alpha \in \mathbb{Z}$  and  $\beta \in \mathcal{C}$  (see [5] and [13], Section 6.5). In fact, we can assume that  $\pi$  satisfies the condition  $\pi(z) = \pi(-z)$ , and throughout the article the notation  $\pi$  is always used for such a morphism.

The commutativity of (4) reduces to the condition  $\varphi(-z) = -\varphi(z)$ . In particular, if  $\beta \neq 0$ , then  $\beta$  is necessarily a point of order two on  $\mathcal{C}$ . Moreover, changing  $\pi(z)$  to  $\pi'(z) = \pi(z + \beta)$ , we see that the condition  $\pi'(z) = \pi'(-z)$  still holds, while (4) holds for  $\varphi' = \alpha z + \beta'$ , where  $\beta' = \alpha\beta$ . Thus, if  $\alpha$  is even, we may assume that  $\beta = 0$ . Notice finally that the complex structure of  $\mathcal{C}$  is completely defined by the conjugacy class of  $A$ , that is if  $A', \mathcal{C}', \pi', \varphi'$  is another collection as above and  $A$  is conjugated to  $A'$ , then  $\mathcal{C}$  is isomorphic to  $\mathcal{C}'$  (see [5] and [13] for more details). Abusing the notation, we will use the term “complex structure corresponding to  $A$ ” meaning the complex structure of  $\mathcal{C}$  from diagram (4).

Assuming that  $\mathcal{C}$  is written in the Weierstrass form

$$\mathcal{C} : y^2 = x^3 + ax + b, \quad a, b \in \mathbb{C}, \quad (5)$$

a prototypical example of a Lattès map is obtained for  $\alpha = 2z$  and  $\pi(x, y) = x$ . In this case,

$$A_{a,b}(z) = \frac{z^4 - 2az^2 - 8bz + a^2}{4z^3 + 4az + 4b}. \quad (6)$$

Equivalently, if  $M$  is a lattice of rank two in  $\mathbb{C}$  such that  $\mathcal{C} = \mathbb{C}/M$ , and  $\wp(z)$  is the corresponding Weierstrass function, then function (6) is defined by the condition  $\wp(2z) = A \circ \wp(z)$ . Taking into account that two functions (6) are conjugated if and only if corresponding elliptic curves are isomorphic, abusing the notation, we will denote by  $\mathcal{L}_j$  any Lattès map (6) with given  $j$ -invariant of curve (5). Thus,  $A_{a,b} = \mathcal{L}_j$ , where

$$j = 1728 \frac{4a^3}{4a^3 + 27b^2}.$$

Let  $F$  be a rational function of degree  $d$ . By definition, the *multiplier spectrum* of  $F$  is a function which assigns to each  $s \geq 1$  the unordered list of multipliers at all  $d^s + 1$  fixed points of  $F^{\circ s}$  taken with appropriate multiplicity. Two rational functions are called *isospectral* if they have the same multiplier spectrum. For example, all the functions from family (6) have the same multiplier spectrum (see e.g. [13]). Nevertheless, by the deep result of McMullen this situation is exceptional (see [3], [5], [13]).

**Theorem 2.1.** (McMullen) *The conjugacy class of any rational function  $F$  which is not a flexible Lattès map is defined up to finitely many choices by its multiplier spectrum.*  $\square$

The notions of equivalence and isospectrality are closely related as the following lemma shows.

**Lemma 2.1.** *Let  $U$  and  $V$  be two rational functions. Then the rational functions  $U \circ V$  and  $V \circ U$  are isospectral.*

*Proof.* Since

$$(U \circ V)^{\circ l}(z_0) = z_0$$

implies that

$$(V \circ U)^{\circ l}(z_1) = z_1,$$

where  $z_1 = V(z_0)$ , the function  $V$  maps periodic points of  $U \circ V$  to periodic points of  $V \circ U$ , and the period of  $V(z_0)$  divides the period of  $z_0$ . Moreover, since  $U$  maps periodic points of  $V \circ U$  to periodic points of  $U \circ V$  as well, and the composition  $U \circ V$  maps bijectively periodic points of  $U \circ V$  of period  $l$  to themselves, we conclude that  $V$  maps bijectively periodic points of  $U \circ V$  of period  $l$  to periodic points of  $V \circ U$  of period  $l$ .

Finally, since by the chain rule

$$((U \circ V)^{\circ l})'(z_0) = ((U \circ V)^{\circ l-1} \circ U)'(z_1) \circ V'(z_0)$$

and

$$((V \circ U)^{\circ l})'(z_1) = V'((U \circ V)^{\circ l-1} \circ U)(z_1) \circ ((U \circ V)^{\circ l-1} \circ U)'(z_1),$$

it follows from

$$((U \circ V)^{\circ l-1} \circ U)(z_1) = z_0$$

that

$$((U \circ V)^{\circ l})'(z_0) = ((V \circ U)^{\circ l})'(z_1). \quad \square$$

**Corollary 2.1.** *Let  $A$  and  $B$  be rational functions such that  $A \sim B$ . Then  $A$  and  $B$  are isospectral.*

*Proof.* By definition,  $A \sim B$  if  $B$  is obtained from  $A$  by a chain of elementary transformations. On the other hand, any such transformation leads to an isospectral function by Lemma 2.1.  $\square$

It is clear that the McMullen theorem combined with Corollary 2.1 proves the “only if” part Theorem 1.1. The case of flexible Lattès maps requires an additional investigation, which is done in the next section.

Notice that isospectral  $A$  and  $B$  are not necessary equivalent. Say, all functions (6) cannot be equivalent since any equivalence class contains at most countably many conjugacy classes. Nevertheless, to our best knowledge all known examples

of isospectral rational functions are obtained either from flexible Lattès maps, or from rigid Lattès maps (see [3], [5], [13]), or else from elementary transformations. Thus, it is still possible that if  $A$  and  $B$  are not Lattès maps, then the fact that  $A$  and  $B$  are isospectral implies that  $A \sim B$ . A comprehensive description of relations between the isospectrality and the equivalence  $\sim$  seems to be a very interesting problem.

Notice also that if  $A$  is a *polynomial*, then the finiteness of  $[A]$  can be established without using the McMullen theorem; see Corollary 5.8 in [10], and also the paper [4] using the notion of “skew twist equivalence” which is essentially coincides with the equivalence  $\sim$  in the setting considered here. The approach of the paper [4] is based on the theory of decomposition of polynomials developed by Ritt [11], while the method of [10] relies on the results of [8] about polynomials sharing preimages of compact sets. However, methods of both these papers are restricted to the polynomial case only.

### 3. EQUIVALENCE CLASSES OF $\mathcal{L}_j$

In order to reduce the number of parameters, in practical calculations we will write elliptic curves in the Legendre form

$$\mathcal{C}_\lambda : y^2 = x(x-1)(x-\lambda), \quad \lambda \in \mathbb{C} \setminus \{0, 1\}, \quad (7)$$

and corresponding functions (6) in the form

$$f_\lambda(z) = \frac{1}{4} \frac{(z^2 - \lambda)^2}{z(z-1)(z-\lambda)}.$$

The curve  $\mathcal{C}_\lambda$  has three subgroups of order two  $G_i$ ,  $i = 1, 2, 3$ , and to each of these groups corresponds an isogeny  $\varphi_i : \mathcal{C}_\lambda \rightarrow \mathcal{C}_i$  with the kernel  $G_i$  (for basic facts about isogenies see e.g. [12], Chapter III). Furthermore, since  $\varphi_i$ ,  $i = 1, 2, 3$ , is a homomorphism, the equality  $\varphi_i(-x) = -\varphi_i(x)$  holds, implying that there exists a rational function  $V_i$  such that the diagram

$$\begin{array}{ccc} \mathcal{C}_\lambda & \xrightarrow{\varphi_i} & \mathcal{C}_i \\ \downarrow \pi_\lambda & & \downarrow \pi_i \\ \mathbb{CP}^1 & \xrightarrow{V_i} & \mathbb{CP}^1 \end{array}$$

is commutative. Finally, for each of the isogenies  $\varphi_i : \mathcal{C}_\lambda \rightarrow \mathcal{C}_i$ ,  $i = 1, 2, 3$ , there exists a dual isogeny  $\widehat{\varphi}_i : \mathcal{C}_i \rightarrow \mathcal{C}_\lambda$  such that

$$\widehat{\varphi}_i \circ \varphi_i = 2z, \quad (8)$$

and a rational function  $U_i$  such that the diagram

$$\begin{array}{ccc} \mathcal{C}_i & \xrightarrow{\widehat{\varphi}_i} & \mathcal{C}_\lambda \\ \downarrow \pi_i & & \downarrow \pi_\lambda \\ \mathbb{CP}^1 & \xrightarrow{U_i} & \mathbb{CP}^1 \end{array}$$

is commutative. Thus, we obtain three decompositions

$$f_\lambda = U_i \circ V_i, \quad i = 1, 2, 3, \quad (9)$$

of the function  $f_\lambda$ . The curves  $\mathcal{C}_i$ ,  $i = 1, 2, 3$ , are defined up to isomorphism only. However, for any isomorphism  $\gamma : \mathcal{C} \rightarrow \tilde{\mathcal{C}}$  between elliptic curves there exists a Möbius transformation such that the diagram

$$\begin{array}{ccc} \mathcal{C} & \xrightarrow{\gamma} & \tilde{\mathcal{C}} \\ \downarrow \pi & & \downarrow \tilde{\pi} \\ \mathbb{CP}^1 & \xrightarrow{\mu} & \mathbb{CP}^1 \end{array}$$

is commutative. Thus, changing in the above construction the curves  $\mathcal{C}_i$  to isomorphic curves we obtain decompositions of  $f_\lambda$  related with decompositions (9) by the transformation

$$U \rightarrow U \circ \mu, \quad V \rightarrow \mu^{-1} \circ V, \quad (10)$$

where  $\mu$  is a Möbius transformation. In fact, decompositions (9) exhaust *all* possible decompositions

$$f_\lambda(z) = U \circ V, \quad \deg V > 1, \quad \deg U > 1, \quad (11)$$

of the function  $f_\lambda$ , considered up transformation (10). More precisely, the following statement holds.

**Lemma 3.1.** *Any decomposition (11) is obtained from some decomposition (9). In more details, any decomposition (11) up to transformation (10) has one of the following three forms:*

$$\begin{aligned} f_\lambda(z) &= \left( z + \frac{\lambda}{z} \right) \circ \left( \frac{1}{4} \frac{z^2 - 4\lambda}{z - \lambda - 1} \right) \\ f_\lambda(z) &= \left( z + \frac{1 - \lambda}{z - 1} \right) \circ \left( \frac{1}{4} \frac{z^2 + 2z + 1}{z + 1 - \lambda} \right) \\ f_\lambda(z) &= \left( z + \frac{\lambda^2 - \lambda}{z - \lambda} \right) \circ \left( \frac{1}{4} \frac{\lambda^2 + 2\lambda z + z^2}{z + \lambda - 1} \right). \end{aligned} \quad (12)$$

*Proof.* Recall that decompositions (11) considered up to transformation (10) correspond to imprimitivity systems of the monodromy group  $\Gamma_\lambda$  of  $f_\lambda$  (see e.g. [6], Section 2.1). Moreover, it is clear that for any decomposition (11) we have  $\deg U = 2$ . Thus, assuming that  $\Gamma_\lambda$  acts on the set  $f_\lambda^{-1}\{c\} = \{z_0, z_1, z_2, z_3\}$ , where  $c$  is a non-critical value of  $f_\lambda(z)$ , decompositions (11) correspond to blocks of size two containing the point  $z_0$ , say. Therefore, there might be at most three such blocks, namely,  $\{z_0, z_1\}$ ,  $\{z_0, z_2\}$ , and  $\{z_0, z_3\}$ .

Explicit expressions for decompositions of  $f_\lambda(z)$  given above can be deduced from Vélú formulas for isogenies (see [14]). These decompositions cannot be obtained one from another by transformation (10) since the corresponding imprimitivity systems are different. Indeed,  $f_\lambda^{-1}\{\infty\} = \{\infty, 0, 1, \lambda\}$ , and blocks containing  $\infty$  corresponding to decompositions (12) are  $\{0, \infty\}$ ,  $\{1, \infty\}$ , and  $\{\lambda, \infty\}$ .  $\square$

**Corollary 3.1.** *Rational functions obtained from  $L_\tau(z)$ ,  $\tau \in \mathbb{C}$ , by an elementary transformation have the form  $A = L_{\tau'}(z)$ ,  $\tau' \in \mathbb{C}$ , where values of  $\tau'$  are defined by the condition that there exists an isogeny  $\mathcal{C}_\tau \rightarrow \mathcal{C}_{\tau'}$  whose kernel is a cyclic group of order two. In particular, if  $A \sim L_\tau(z)$ ,  $\tau \in \mathbb{C}$ , then  $A$  is conjugated to  $L_{\tau'}(z)$  for some  $\tau' \in \mathbb{C}$ .*

*Proof.* Indeed, if  $f_\lambda = U \circ V$  is a decomposition such that one of the functions  $U$  and  $V$  is invertible, then the corresponding elementary transformation leads to a function conjugate to  $f_\lambda$ . On the other hand, since any decomposition (11) is obtained from decomposition (8), all other elementary transformations of  $f_\lambda$  are projections of the isogenies

$$\varphi_i \hat{\varphi}_i : \mathcal{C}_i \rightarrow \mathcal{C}_i, \quad i = 1, 2, 3.$$

Now the corollary follows from the following property of isogenies: if  $\varphi : \mathcal{C} \rightarrow \hat{\mathcal{C}}$  is an isogeny and  $\hat{\varphi} : \hat{\mathcal{C}} \rightarrow \mathcal{C}$  is its dual, then  $\varphi \circ \hat{\varphi} = 2z$  on  $\hat{\mathcal{C}}$ .  $\square$

Notice that the images of the isogenies  $\varphi_i : \mathcal{C}_\lambda \rightarrow \mathcal{C}_i$ ,  $i = 1, 2, 3$ , corresponding to left parts of decompositions (12) do not have Legendre form (7). So, elementary transformations corresponding to decompositions (12) are not *equal* to functions  $f_{\lambda'}(z)$  but only *conjugate* to such functions.

Recall that if  $\mathcal{C}_j$  and  $\mathcal{C}_{j'}$  are two elliptic curves with  $j$ -invariant  $j$  and  $j'$ , then an isogeny  $\mathcal{C}_j \rightarrow \mathcal{C}_{j'}$  whose kernel is a cyclic group of order two exists if and only if  $(j, j')$  is a point on the classical modular curve  $\Phi_2(x, y) = 0$ , which can be seen as a model of the algebraic curve  $\mathbb{H}/\Gamma_0(2)$  (see e.g. [2], Chapter 5, or [12], Appendix C). Thus, Corollary 3.1 implies Theorem 1.2. Furthermore, since  $\Phi_2(x, y) = 0$  is given by the equation

$$\begin{aligned} & -x^2y^2 + x^3 + y^3 + 2^4 \cdot 3 \cdot 31xy(x+y) + 3^4 \cdot 5^3 \cdot 4027xy \\ & - 2^4 \cdot 3^4 \cdot 5^3(x^2 + y^2) + 2^8 \cdot 3^7 \cdot 5^6(x+y) - 2^{12} \cdot 3^9 \cdot 5^9 = 0, \end{aligned} \quad (13)$$

which can be parametrized by the rational functions

$$x = 64 \frac{(j+4)^3}{j^2}, \quad y = 64 \frac{(j+4)^3}{j^2} \circ \frac{1}{j},$$

the correspondence  $\mathcal{F}$  associated with (13) has form (3). Notice that the correspondence  $\mathcal{F}$  is symmetric in accordance with the fact that  $\sim$  is an equivalence relation. In particular, the forward orbit of any point coincides with the backward one.

It is not immediately clear from (13) that the orbit of any  $j$  is infinite. Moreover, there exist correspondences  $F(x, y) = 0$  with  $\deg_y F > 1$  having points with finite orbits (the condition  $\deg_y F > 1$  assures that iterations of  $\mathcal{F}$  do not reduce to usual iterations of some rational function). For example, the orbit of the point  $\frac{1}{\sqrt{2}}$  under the correspondence

$$x^2 + y^2 = 1$$

consists of two points.

In order to show that  $[\mathcal{L}_j]$  contains infinitely many conjugacy classes we will use analytic properties of the elliptic modular function  $j(\tau)$  considered as a modular function of weight zero for  $SL(2, \mathbb{Z})$  on the upper half-plane. Thus, we use the symbol  $j$  in both possible contexts: as the value of the modular function  $j(\tau)$ , and as the  $j$ -invariant of the elliptic curve isomorphic to the  $\mathbb{C}/L_\tau$ , where  $L_\tau = \langle 1, \tau \rangle$ ,  $\tau \in \mathbb{H}$ , is a normalized lattice.

For a normalized lattice  $L_\tau = \langle 1, \tau \rangle$ ,  $\tau \in \mathbb{H}$ , its normalized 2-isogenous lattices, up to isomorphism, are  $L_{\tau/2}$ ,  $L_{2\tau}$ ,  $L_{\frac{1+\tau}{2}}$ . The corresponding isogenies and dual isogenies are

$$L_\tau \xrightarrow{z} L_{\tau/2}, \quad L_\tau \xrightarrow{2z} L_{2\tau}, \quad L_\tau \xrightarrow{z} L_{\frac{1+\tau}{2}},$$

and

$$L_{\tau/2} \xrightarrow{2z} L_{\tau}, \quad L_{2\tau} \xrightarrow{z} L_{\tau}, \quad L_{\frac{1+\tau}{2}} \xrightarrow{2z} L_{\tau}.$$

Thus, the orbit of  $j(\tau)$  in  $\mathbb{C}$  under correspondence (13) is the  $j$ -image of the orbit of  $\tau$  in  $\mathbb{H}$  under the action of the group generated by the transformations

$$\tau \rightarrow 2\tau, \quad \tau \rightarrow \frac{1+\tau}{2},$$

and hence in order to prove that the orbit of  $j(\tau)$  is infinite it is enough to show that for any  $\tau \in \mathbb{H}$  the sequence  $j(2^k \tau)$ , say, takes infinitely many distinct values.

The Fourier expansion for  $j(\tau)$  in  $q = e^{2\pi i \tau}$  is

$$j(\tau) = \frac{1}{q} + 744 + 196884q + \dots$$

Further,

$$q_k = e^{2\pi i(2^k \tau)} \rightarrow 0, \quad \text{as } k \rightarrow \infty,$$

since  $\Im(\tau) > 0$ . Therefore,

$$j(2^k \tau) \rightarrow \infty, \quad \text{as } k \rightarrow \infty,$$

implying that  $j(2^k \tau)$  takes infinitely many distinct values. This proves the “if” part of Theorem 1.1 for functions  $\mathcal{L}_j$ .

Prove now Theorem 1.1 for arbitrary flexible Lattès maps. Assume first that the function  $\varphi$  in (4) has the form  $\varphi = \alpha z$ ,  $\alpha \in \mathbb{Z}$ , and denote the corresponding Lattès map by  $A_0$ . It is not true anymore that any decomposition of  $A_0$  is obtained from cyclic  $\alpha$ -isogenies. For example, if  $\alpha$  is composite,  $\alpha = \alpha_1 \alpha_2$ , we obviously can decompose  $A_0$  into a composition of flexible Lattès maps of degrees  $\alpha_1^2$  and  $\alpha_2^2$ . Nevertheless, to any pair of cyclic  $\alpha$ -isogenies  $\psi : \mathcal{C} \rightarrow \mathcal{C}'$  and  $\hat{\psi} : \mathcal{C}' \rightarrow \mathcal{C}$  with

$$\hat{\psi} \circ \psi = \alpha z \tag{14}$$

corresponds a decomposition of  $A_0$ , whose elementary transformation is again a flexible Lattès map, and in order to prove that  $[A_0]$  has infinitely many conjugacy classes it is enough to prove that we can obtain infinitely many conjugacy classes using elementary transformations arising from decompositions (14) only. In turn, for this purpose it is enough to show arguing as above that for any  $\tau \in \mathbb{H}$  the sequence  $j(\alpha^k \tau)$  takes infinitely many values.

The case  $\varphi = \alpha z + \beta$ , where  $\alpha \in \mathbb{Z}$  is odd and  $\beta$  is a point of order two can be reduced to the previous one as follows. Set  $\varphi_\alpha = \alpha z$  and  $\varphi_\beta = z + \beta$ . Clearly, both  $\varphi_\alpha$  and  $\varphi_\beta$  map  $\mathcal{C}$  to itself and satisfy

$$\varphi = \varphi_\beta \circ \varphi_\alpha = \varphi_\alpha \circ \varphi_\beta. \tag{15}$$

Further, since  $\varphi_\beta(-z) = -\varphi_\beta(z)$ , there exists a Möbius transformation  $\mu$  which makes the diagram

$$\begin{array}{ccc} \mathcal{C} & \xrightarrow{\varphi_\beta} & \mathcal{C} \\ \downarrow \pi & & \downarrow \pi \\ \mathbb{CP}^1 & \xrightarrow{\mu} & \mathbb{CP}^1 \end{array}$$

commutative. Therefore, the flexible Lattès map  $A$  corresponding to  $\varphi = \alpha z + \beta$  and flexible Lattès map  $A_0$  corresponding to  $\varphi = \alpha z$  satisfy the equality

$$A = \mu \circ A_0 = A_0 \circ \mu \tag{16}$$



for some Möbius transformation  $\mu$ . Moreover, complex structures corresponding to  $A$  and  $A_0$  coincide.

Consider now a decomposition  $A_0 = U \circ V$  obtained from (14) and its elementary transformation  $A_0^1 = V \circ U$ . Clearly, the elementary transformation  $A_0 \rightarrow A_0^1$  induces the elementary transformation

$$A = \mu \circ U \circ V \rightarrow A^1 = V \circ \mu \circ U.$$

Furthermore, changing  $\mathcal{C}'$  to an isomorphic curve, we can assume that

$$\psi = z, \quad \hat{\psi} = \alpha z,$$

implying that the compositions

$$\mathcal{C} \xrightarrow{\varphi_\beta} \mathcal{C} \xrightarrow{\psi} \mathcal{C}'$$

and

$$\mathcal{C} \xrightarrow{\psi} \mathcal{C}' \xrightarrow{\varphi_\beta} \mathcal{C}'$$

are equal. Considering now the commutative diagram

$$\begin{array}{ccccccc} \mathcal{C}' & \xrightarrow{\hat{\psi}} & \mathcal{C} & \xrightarrow{\varphi_\beta} & \mathcal{C} & \xrightarrow{\psi} & \mathcal{C}' \\ \downarrow \pi' & & \downarrow \pi & & \downarrow \pi & & \downarrow \pi' \\ \mathbb{CP}^1 & \xrightarrow{U} & \mathbb{CP}^1 & \xrightarrow{\mu} & \mathbb{CP}^1 & \xrightarrow{V} & \mathbb{CP}^1 \end{array}$$

we see that

$$A^1 = (V \circ \mu) \circ U = \mu_1 \circ V \circ U = \mu_1 \circ A_0^1$$

for some Möbius transformation  $\mu_1$

It is clear that continuing in this way we obtain, starting from a chain of elementary transformations

$$A_0 \rightarrow A_0^1 \rightarrow A_0^2 \rightarrow \dots, \quad (17)$$

a chain of elementary transformations

$$A \rightarrow A^1 \rightarrow A^2 \rightarrow \dots. \quad (18)$$

Moreover, since the complex structures corresponding to  $A_i^0$  and  $A_i$  coincide, whenever the number of complex structures corresponding to (17) is infinite, the same is true for (18). This finishes the proof of Theorem 1.1.

## REFERENCES

1. F. Klein, *Ueber die Transformation der elliptischen Functionen und die Auflösung der Gleichungen fünften Grades*, Math. Ann., 14 (1879) 111-172.
2. S. Lang, *Elliptic functions*, Graduate Texts in Mathematics, 112. Springer-Verlag, New York, 1987.
3. C. McMullen, *Families of rational maps and iterative root-finding algorithms*, Ann. of Math., 125, No. 3 (1987), 467-493.
4. A. Medvedev, T. Scanlon, *Invariant varieties for polynomial dynamical systems*, Annals of Mathematics, 179 (2014), no. 1, 81 - 177.
5. J. Milnor, *On Lattès maps*, Dynamics on the Riemann Sphere. Eds. P. Hjorth and C. L. Petersen. A Bodil Branner Festschrift, European Mathematical Society, 2006, pp. 9-43.
6. M. Muzychuk, F. Pakovich, *Jordan-Holder theorem for imprimitivity systems and maximal decompositions of rational functions*, Proc. Lond. Math. Soc., 102 (2011), no. 1, 1-24.
7. J. Milnor, *Dynamics in one complex variable*, Princeton Annals in Mathematics 160. Princeton, NJ: Princeton University Press (2006).
8. F. Pakovich, *On polynomials sharing preimages of compact sets, and related questions*, Geom. Funct. Anal., 18, No. 1, 163-183 (2008).

9. F. Pakovich, *On semiconjugate rational functions*, Geom. Funct. Anal. 26, no. 4, 1217-1243 (2016).
10. F. Pakovich, *Polynomial semiconjugacies, decompositions of iterations, and invariant curves*, Ann. Sc. Norm. Super. Pisa Cl. Sci., to appear.
11. J. Ritt, *Prime and composite polynomials*, American M. S. Trans. 23, 51-66 (1922).
12. J. Silverman, *The arithmetic of elliptic curves. Graduate Texts in Mathematics*, 106. Springer-Verlag, New York, 1986.
13. J. Silverman, *The arithmetic of dynamical systems*, Graduate Texts in Mathematics, 241. Springer, New York, 2007.
14. J. Vélu, *Isogénies entre courbes elliptiques*, C. R. Acad. Sci. Paris Sr. A-B 273 (1971), A238-A241.